549,408

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 September 2004 (30.09.2004)

PCT

(10) International Publication Number
WO 2004/084458 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number:
PCT/US2004/007403

(22) International Filing Date: 11 March 2004 (11.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/454,542 14 March 2003 (14.03.2003) US

(71) Applicant *(for all designated States except US)*: **THOMSON LICENSING S.A.** [FR/FR]; 46, Quai A. Le Gallo, F-92648 Boulogne (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ZHANG, Junbiao** [CN/US]; 20 Jenna Drive, Bridgewater, NJ 08807 (US). **MATHUR, Saurabh** [IN/US]; 4923 Quail Ridge Drive, Plainsboro, IN 08536 (US). **MODY, Sachin** [IN/US]; 708 White Pine Circle, Lawrenceville, NJ 08648 (US).

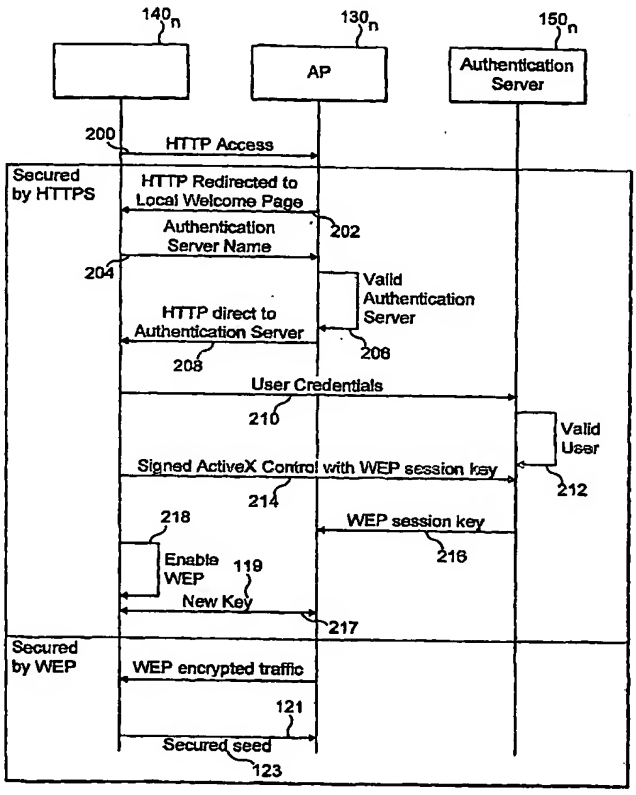
(74) Agents: **TRIPOLI, Joseph** et al.; c/o Thomson Licensing, Inc., Two Independence Way, Suite 200, Princeton, New Jersey 08540 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK,

[Continued on next page]

(54) Title: WLAN SESSION MANAGEMENT TECHNIQUES WITH SECURE REKEYING AND LOGOFF



(57) Abstract: The invention provides a method for improving the security of a mobile terminal in a WLAN environment by installing two shared secrets instead of one shared secret, the initial session key, on both the wireless user machine and the WLAN access point during the user authentication phase. One of the shared secrets is used as the initial session key and the other is used as a secure seed. Since the initial authentication is secure, these two keys are not known to a would be hacker. Although the initial session key may eventually be cracked by the would be hacker, the secure seed remains secure as it is not used in any insecure communication.

WO 2004/084458 A2

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.